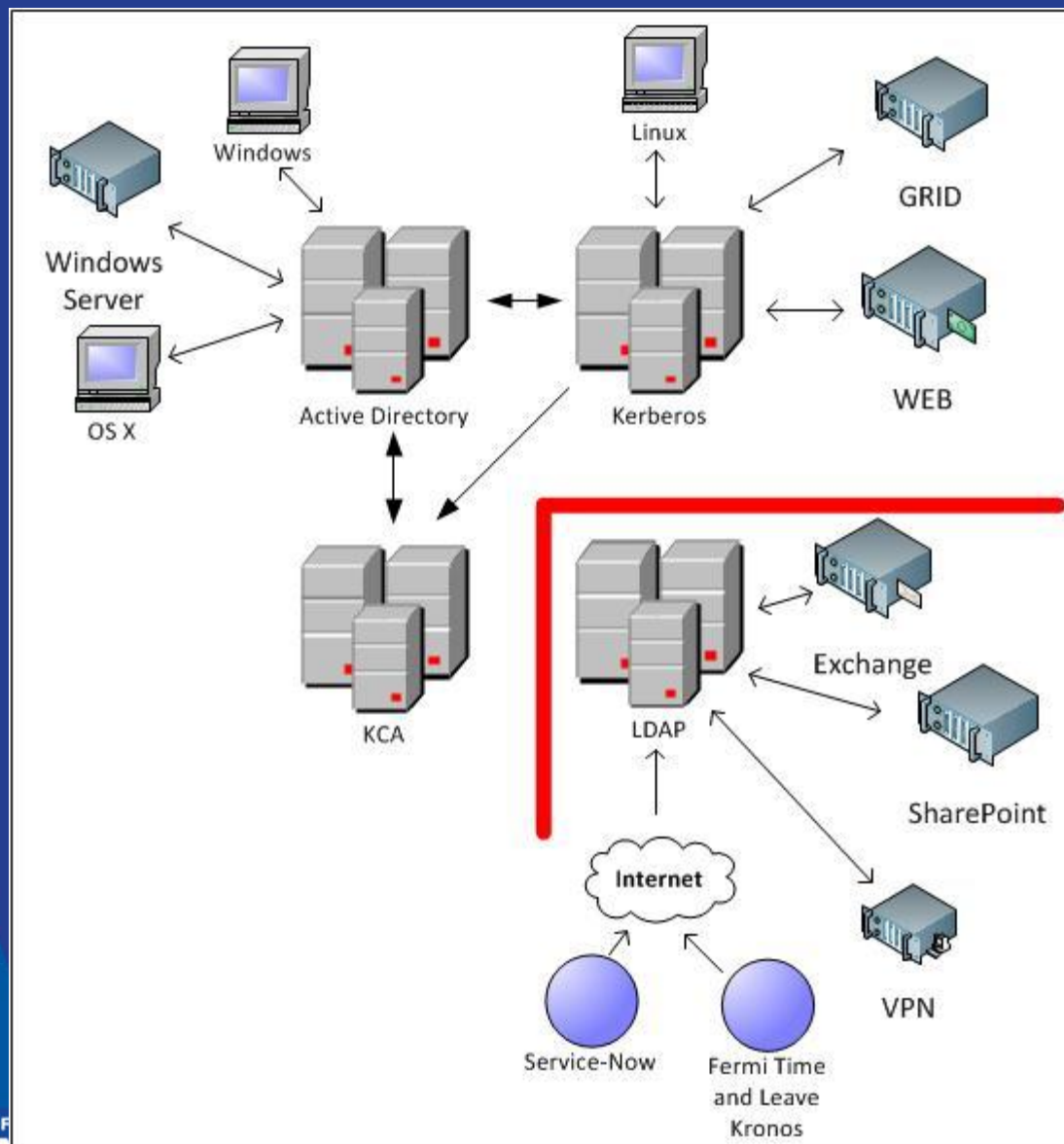


Authentication at Fermilab

Fermilab supports several authentication mechanisms for user and computer authentication. This talk will cover our authentication systems, design considerations, and using them as designed in our diverse environment.

Centralized Authentication Environment



U.S. DEPARTMENT OF
ENERGY

Fermilab

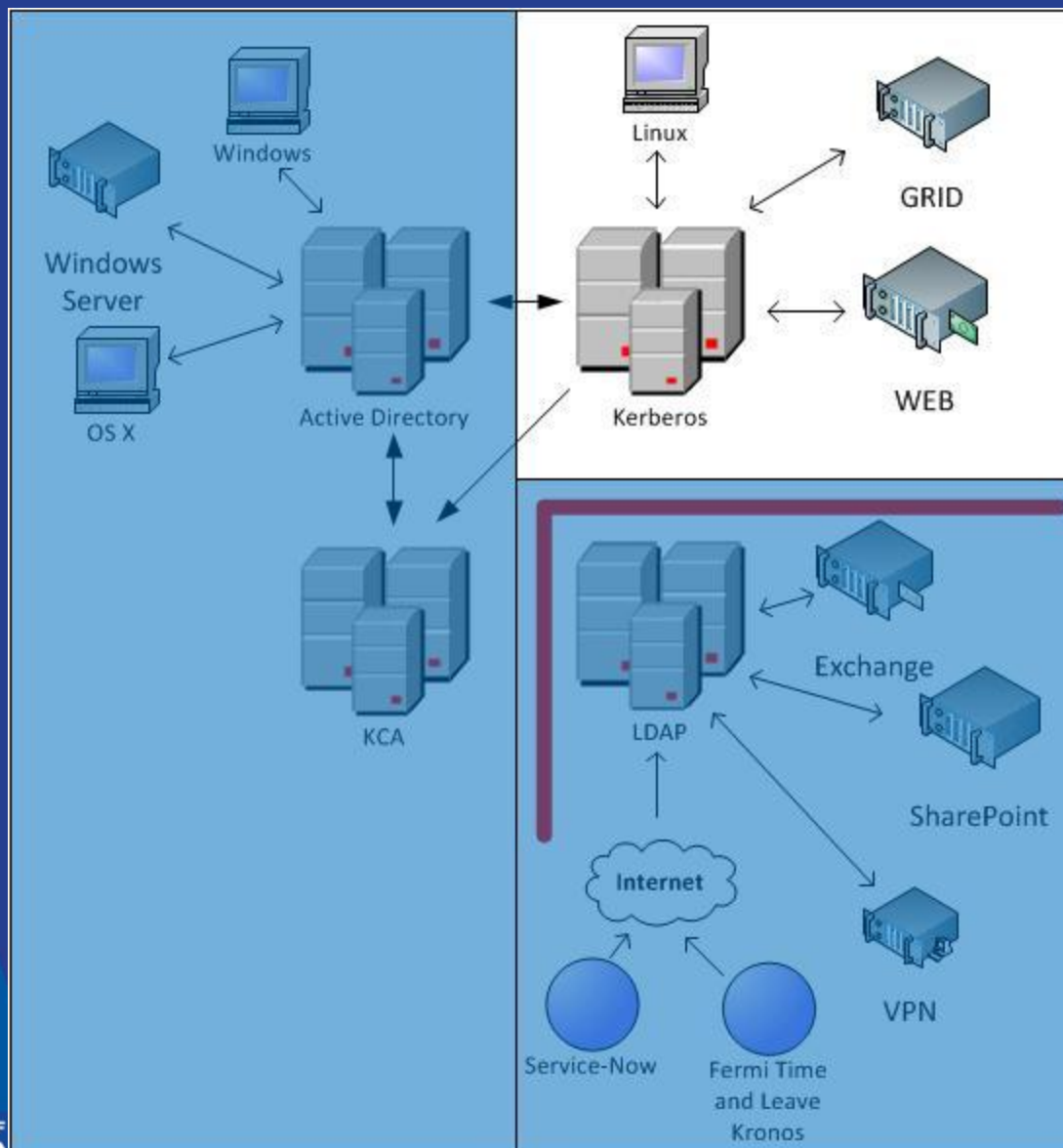
Three Authentication Services?

- 1999 - The Kerberos realm was our initial centralized authentication service
- 2001 - Active Directory was implemented to collapse several NT domains
- 2009 – LDAP was implemented to centralize authentication for the growing number of web apps that could use LDAP for authentication
- Together these services provide a secure, centralized solution that serves the needs of the varied communities and applications at Fermilab.

The Authentication Environment

- Designing, operating and maintaining authentication mechanisms to meet diverse needs of the user community at a national laboratory is challenging
- We have to balance the needs for scientific computing with the needs for traditional computing
- The solutions must be scalable and secure
- We have to keep in mind that our real business is science

Kerberos



Kerberos

- The Kerberos realm is used for scientific computing
 - Workstations
 - Servers
 - Farm nodes
 - GRID nodes
- A Kerberos realm allows for centralized management of users on *nix based platforms.
 - Linux
 - Solaris
 - HP/UX
 - OS X



Kerberos Principals

Total 75841				
Compound 64078				
host/	18295		/cd/	678
ftp/	18203		enstore/cd/	635
/cdf/	14452		/d0/	464
/cdf/*caf	12757		/bd/	285
/cron/	3344		/ft/farm	84
/cms/farm	1477			
Active Users	3658			
Computers	18274			

Fermilab's Kerberos infrastructure is based on the MIT distribution and issues 10 million tickets per week

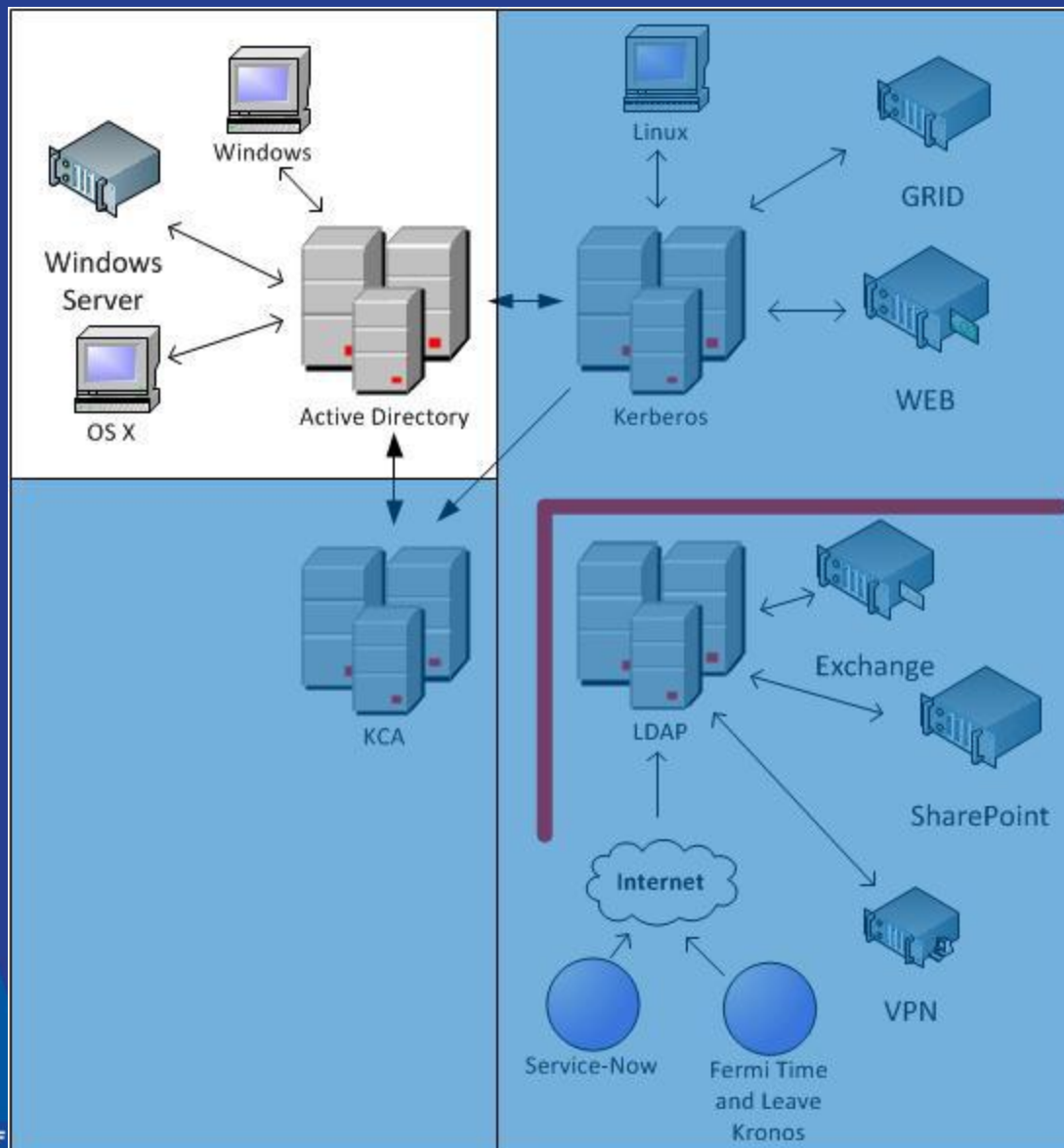
Kerberos Security Considerations

- Minimal number of Kerberos Administrator accounts
- Administrator access is restricted to tightly controlled servers
- Delegated administration tasks are restricted to special accounts

Kerberos Auditing

- One reporting tool in use
 - syslogNG
 - Two instances
 - Kerberos Administrators
 - Computer Security Team
- Special notifications for user account creation, account enable, and deletion

Active Directory (AD)



Active Directory



- AD is used for traditional computing
 - HR, ES&H, FESS
- Logon services for Windows workstations
- File and print services
- Windows integrated applications
- Growing number of OS X systems participating in the domain

Active Directory Risk Assessment

- Fermilab hosted Microsoft Professional Services for an Active Directory Risk Assessment in 2011
 - Overall results were very good
 - Engineer noted the low number of DA accounts was well below the normal encountered
 - Complimented the configuration for delegated AD object management.

Active Directory

	Total	Enabled	Active
Users	12900	5400	3000

Workstations			Servers	
XP	1047		WS 2000	1
Vista	14		WS 2003	167
Windows 7	1852		WS 2008	154
OS/X	167			

Active Directory Security Considerations

- Minimal number of Domain Administrator (DA) accounts
 - DA access is restricted to tightly controlled servers
- Delegated AD administration is restricted to special accounts
 - Server administration is restricted to special accounts
 - Minimizing local administrator access on workstations

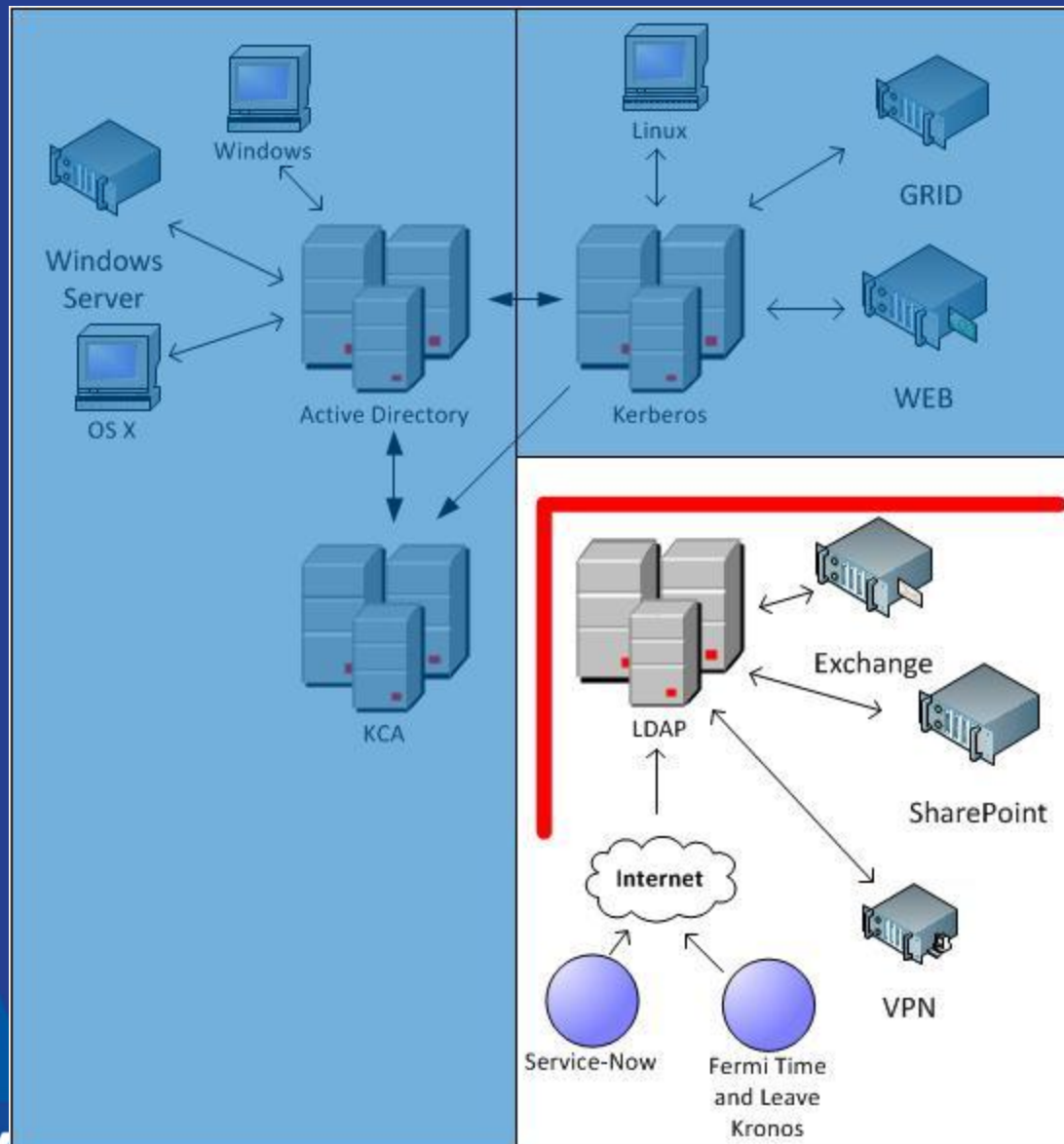
Active Directory Security Considerations

- Centralized Anti-Virus Management
 - Symantec
 - Sophos
- Centralized Patch Management
 - Windows Software Update Services (WSUS)
 - System Center Configuration Manager (SCCM)
 - Apple Software Update Server (ASUS)
- Centralized Configuration Management
 - System Center Configuration Manager
 - Casper

Active Directory Auditing

- Two reporting tools in place
 - Quest Change Auditor
 - Domain Administrators
 - syslogNG
 - Computer Security Team
- Special notifications for user account creation, user account enable, and user account deletion

LDAP



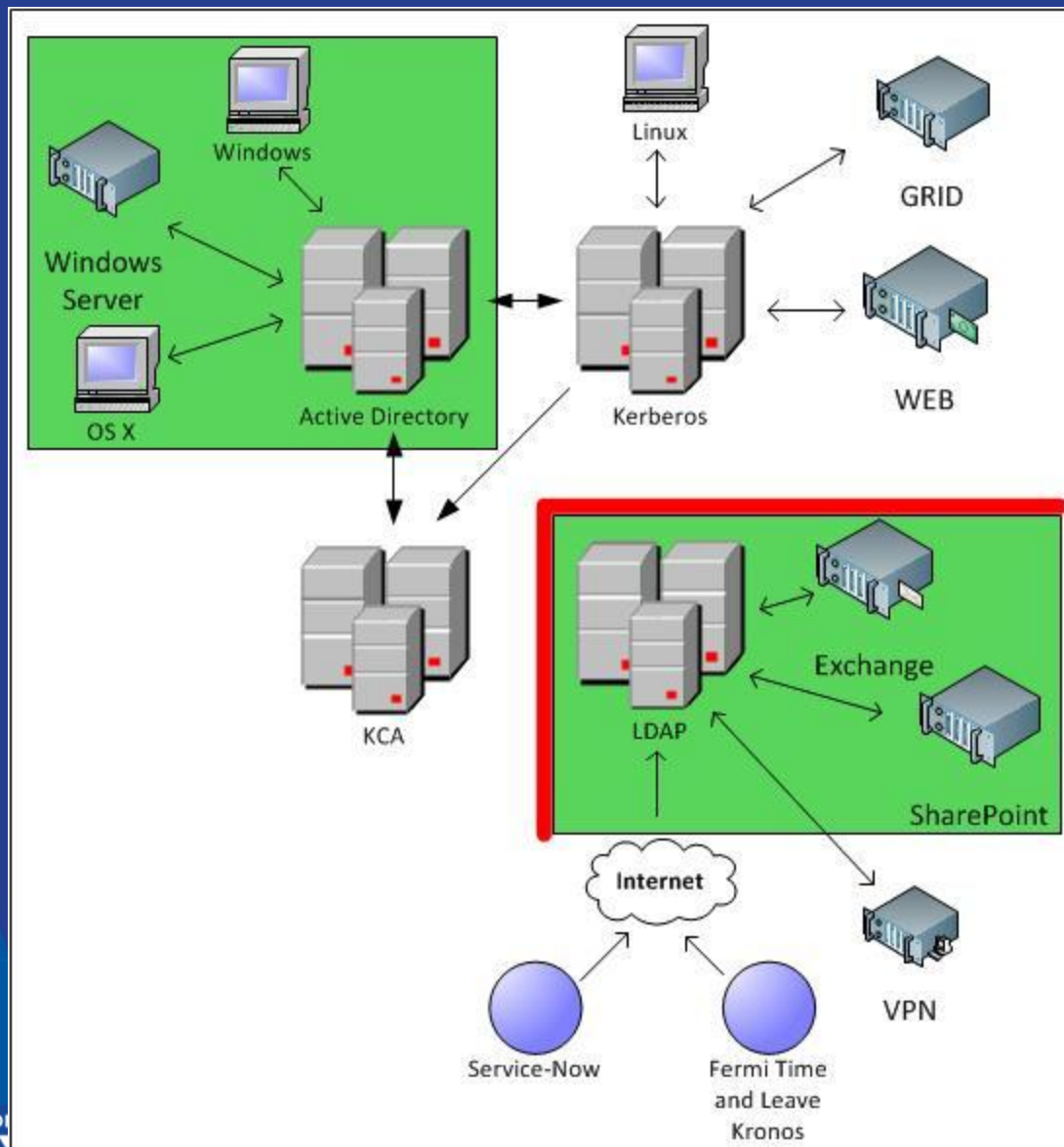
LDAP

- LDAP over SSL authentication
- Supports applications hosted at Fermilab
 - SharePoint
 - Exchange Email and Calendar
 - VPN
- And those hosted in the cloud
 - Service-Now
 - Kronos Time and Leave

LDAP

- Based on Active Directory
 - 13000 User Accounts
 - 5400 Active Users

LDAP Security Considerations



U.S. DEPARTMENT OF
ENERGY

Fermilab

LDAP Security Considerations

- The LDAP service is NOT part of the forest used for AD
- There is NO trust relationship with the forest used for AD
 - Part of the design
 - Separate passwords to contain issues resulting from compromise of user passwords

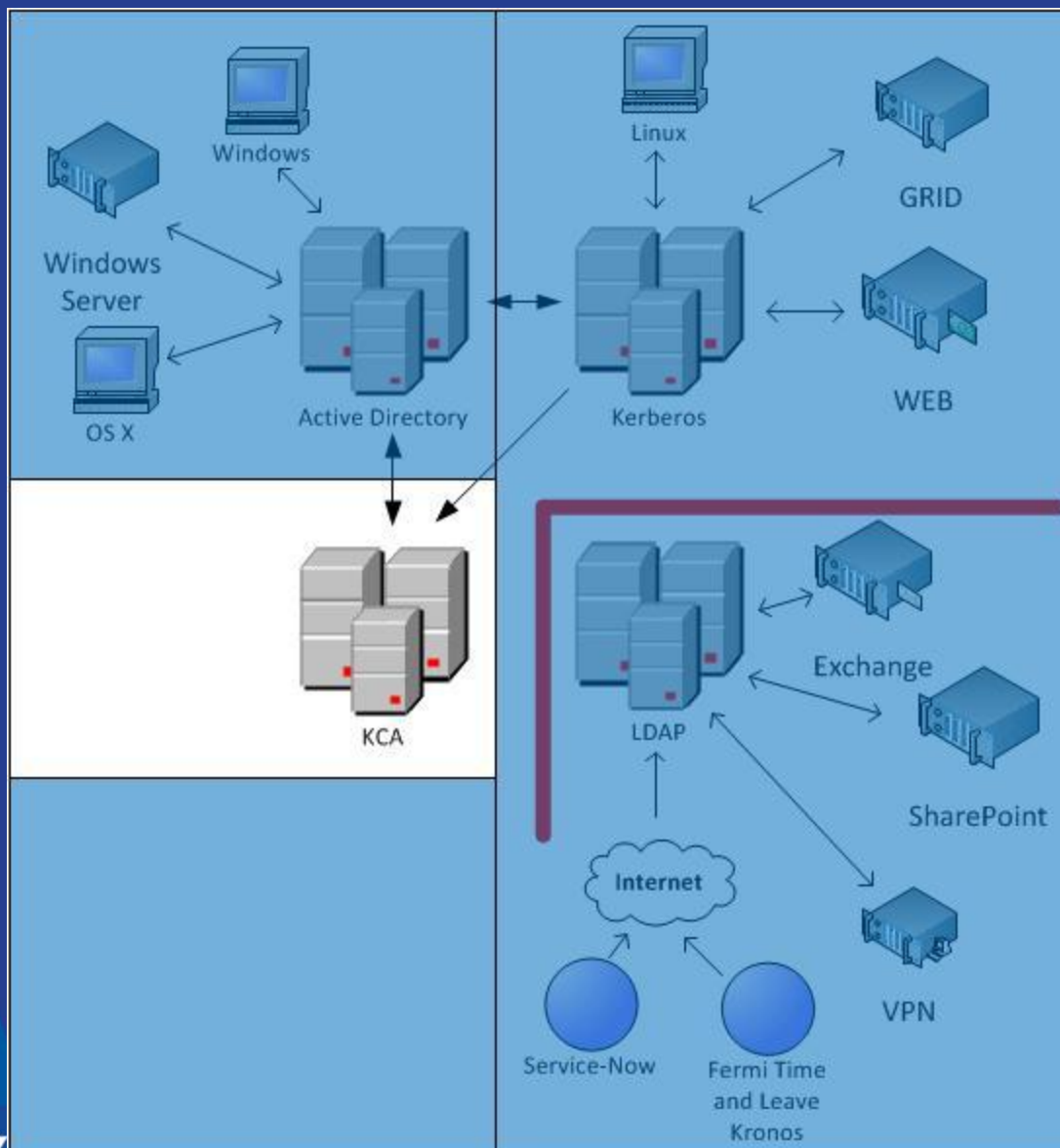
LDAP Security Considerations

- Active Directory supports LDAP so why create a unique LDAP service based on a different Active Directory forest?
 - Unique security rules for interactive Kerberos environments
 - AD uses Kerberos for authentication so we treat it as a Kerberos infrastructure
 - E-Mail passwords tend to be used on public (i.e. Starbucks, hotels, etc) WiFi networks and are susceptible to being compromised

LDAP Security Considerations

- By separating the LDAP service from the AD service (email from interactive) we feel we are lowering the risk of interactive passwords being compromised
- If a LDAP password is compromised E-Mail and SharePoint access can be impacted. Access to Kerberos based scientific applications, data, PII and business applications located in Active Directory are not impacted.

Kerberos Certificate Authority (KCA)



Kerberos Certificate Authority

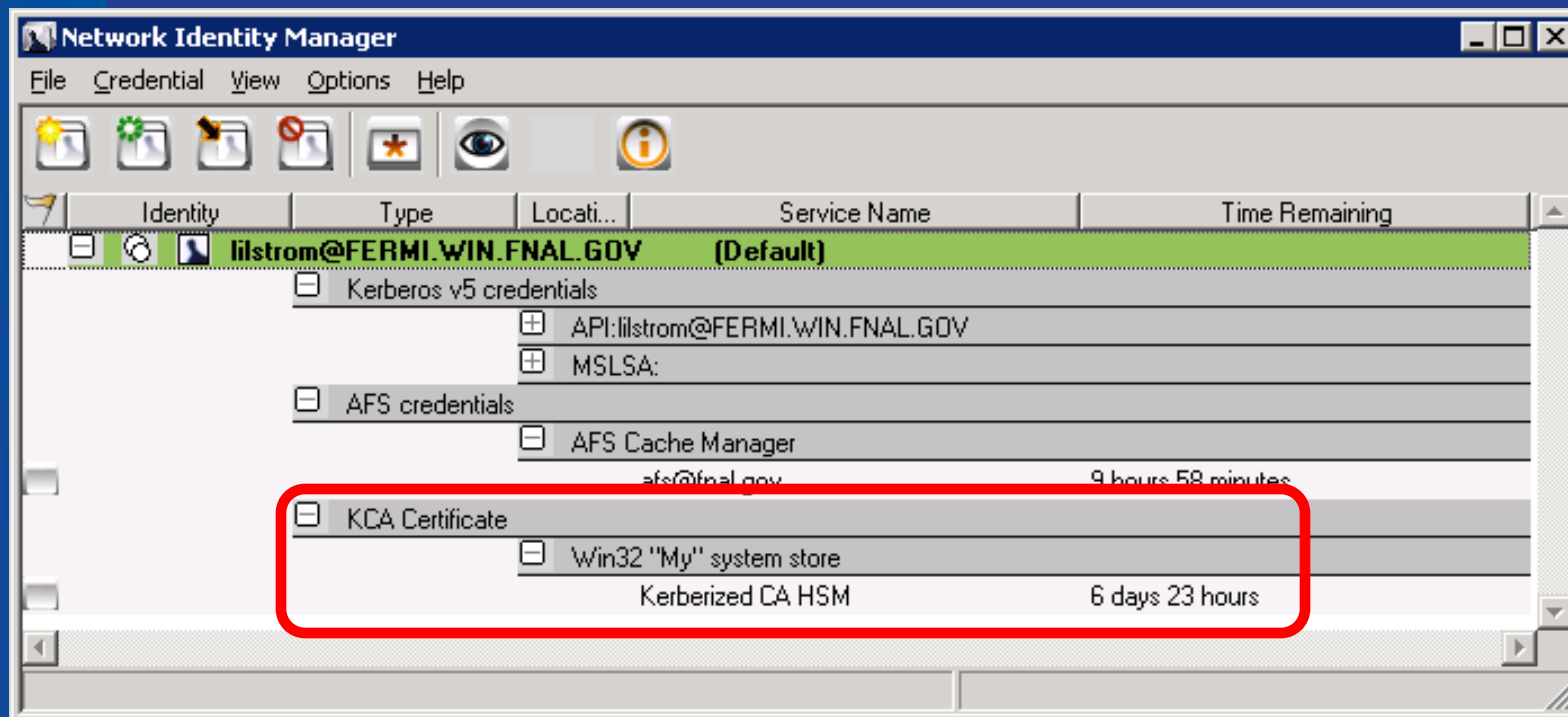
- Open source application running on Windows Server
 - Issues 80,000 certificates per week
- Provides short lifetime x.509 certificates for accessing web services
 - Maximum lifetime of 7 days
- Certificates are issued after authentication from Active Directory or Kerberos

KCA Certificate Usage

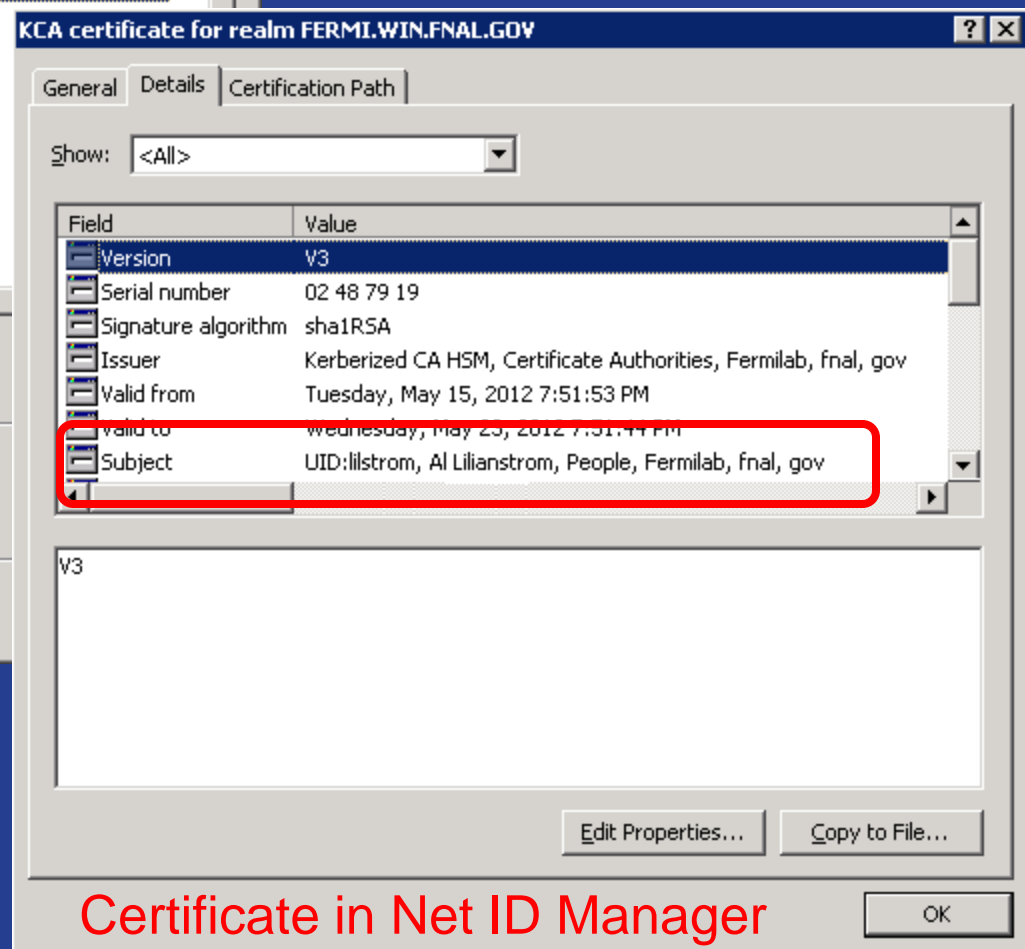
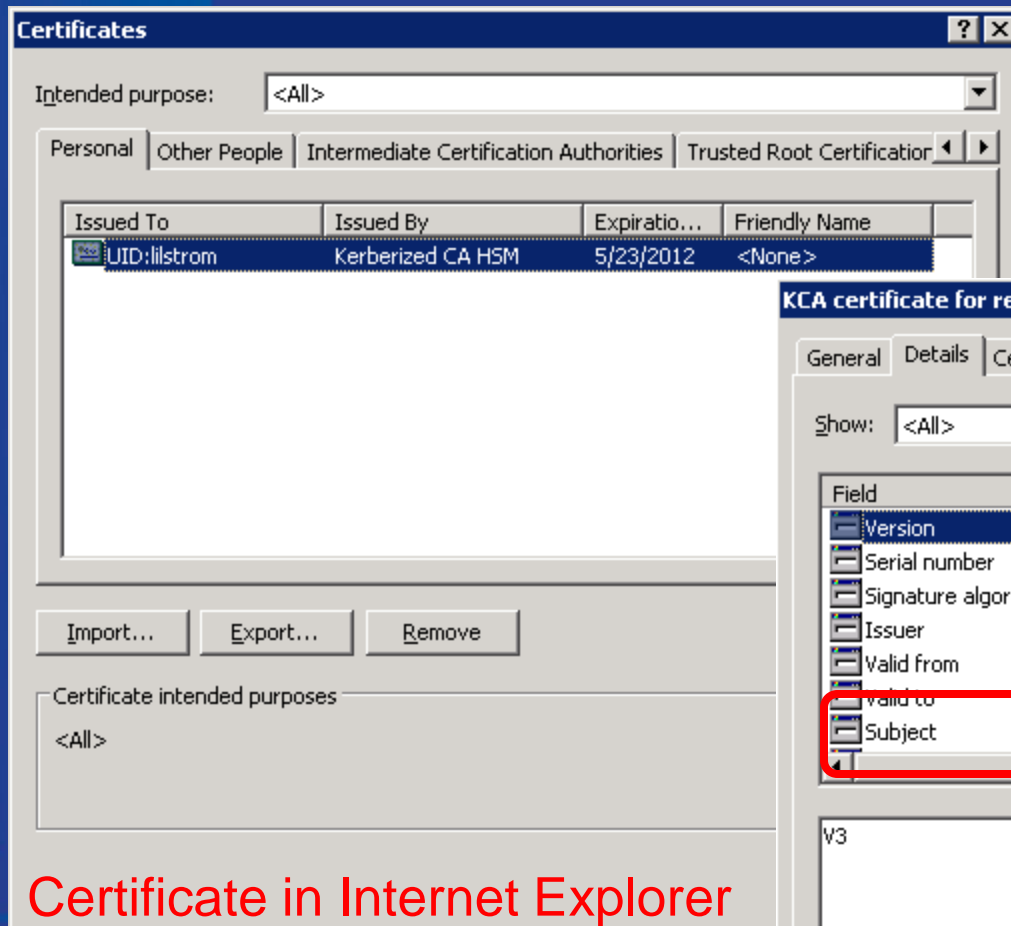
- Web page authorization
 - Leave Usage
 - Document Database
 - Training Requirements
- GRID resources
 - Access to GRID Virtual systems
 - GRID job submission
- **** Not used for signing email ****

KCA Tools - Windows

- Open source Net ID Manager client used on Windows systems to automatically acquire x.509 certificate at logon



KCA Tools - Windows



KCA Tools – OS X and *nix

- Scripts and utilities are provided to OS X and *nix users to acquire x.509 certificates as needed
- Certificates are inserted in to the default browsers on each OS via the script

KCA Tools – OS X and *nix

```
lilstrom@creamskimmer:~  
[lilstrom@creamskimmer ~]$ klist  
Ticket cache: FILE:/tmp/krb5cc_9290_gYJgW30880  
Default principal: lilstrom@FERMI.WIN.FNAL.GOV  
  
Valid starting      Expires            Service principal  
05/17/12 08:12:36   05/17/12 17:26:11  krbtgt/FERMI.WIN.FNAL.GOV@FERMI.WIN.FNAL.GOV  
renew until 05/24/12 07:26:11  
05/17/12 08:13:34   05/17/12 17:26:11  afs/fnal.gov@FERMI.WIN.FNAL.GOV  
renew until 05/24/12 07:26:11  
  
Kerberos 4 ticket cache: /tmp/tkt9290  
klist: You have no tickets cached  
[lilstrom@creamskimmer ~]$
```

```
lilstrom@creamskimmer:~  
[lilstrom@creamskimmer ~]$ get-cert -i  
Get-Cert V3.1 Linux 261009  
Option selected to obtain KCA certificates and attempt to auto-import into Mozilla and Firefox  
Found existing certificate. Deleting...  
Imported certificate to /home/lilstrom/.mozilla/firefox/mbg7dwo0.default  
  
Fermilab KCA certificate imported into browsers  
  
If you need to manually import the certificate into other applications, you can find the converted certificates at:  
  
x509 format: /tmp/x509up_u9290  
PKCS12 format: /tmp/x509up_u9290.p12  
  
[lilstrom@creamskimmer ~]$
```

KCA Tools – OS X and *nix

```
lilstrom@creamskimmer:~  
[lilstrom@creamskimmer ~]$ klist  
Ticket cache: FILE:/tmp/krb5cc_9290_gYJgW30880  
Default principal: lilstrom@FERMI.WIN.FNAL.GOV  
  
Valid starting      Expires            Service principal  
05/17/12 08:12:36   05/17/12 17:26:11  krbtgt/FERMI.WIN.FNAL.GOV@FERMI.WIN.FNAL.GOV  
    renew until 05/24/12 07:26:11  
05/17/12 08:13:34   05/17/12 17:26:11  afs/fnal.gov@FERMI.WIN.FNAL.GOV  
    renew until 05/24/12 07:26:11  
05/17/12 08:16:33   05/17/12 17:26:11  krbtgt/WIN.FNAL.GOV@FERMI.WIN.FNAL.GOV  
    renew until 05/24/12 07:26:11  
05/17/12 08:16:33   05/17/12 17:26:11  krbtgt/FNAL.GOV@WIN.FNAL.GOV  
    renew until 05/24/12 07:26:11  
05/17/12 08:16:36   05/17/12 17:26:11  kca_service/winserver2.fnal.gov@FNAL.GOV  
    renew until 05/24/12 07:26:11  
05/16/12 14:16:36   05/24/12 13:26:11  kx509/certificate@  
  
Kerberos 4 ticket cache: /tmp/tkt9290  
klist: You have no tickets cached  
[lilstrom@creamskimmer ~]$
```

KCA Tools – OS X and *nix

```
lilstrom@creamskimmer:~  
[lilstrom@creamskimmer ~]$ openssl x509 -in /tmp/x509up_u9290 -text  
Certificate:  
  Data:  
    Version: 3 (0x2)  
    Serial Number: 38309865 (0x2488fe9)  
    Signature Algorithm: sha1WithRSAEncryption  
    Issuer: DC=gov, DC=fnal, O=Fermilab, OU=Certificate Authorities, CN=Kerberized  
  CA HSM  
  Validity  
    Not Before: May 16 13:16:36 2012 GMT  
    Not After : May 24 12:26:11 2012 GMT  
    Subject: DC=gov, DC=fnal, O=Fermilab, OU=People, CN=Al Lilianstrom, CN=UID:lil  
strom  
  Subject Public Key Info:  
    Public Key Algorithm: rsaEncryption  
    RSA Public Key: (1024 bit)  
      Modulus (1024 bit):  
        00:d5:d5:1f:3a:90:45:66:16:5b:83:58:4d:2d:b2:  
        de:b3:99:b1:b6:e7:b4:5a:97:f9:d7:a6:13:00:bd:  
        cc:b7:78:6a:f8:47:3f:c4:8a:2b:4f:14:e9:8a:cb:  
        b2:84:0a:ce:e7:57:90:88:29:54:74:93:46:c7:ae:  
        fc:41:37:6e:86:89:1f:7c:96:f9:71:05:bf:13:da:  
        5d:e3:f9:e8:66:87:32:be:a9:e8:62:1b:c3:6c:27:  
        03:ac:bd:c9:a3:0f:5a:02:3a:7c:5b:f6:ea:a8:ad:  
        43:9e:e9:65:e0:61:fe:1e:91:c7:77:4a:f1:3a:59:  
        30:8b:11:4a:a1:17:61:c7:59  
      Exponent: 65537 (0x10001)  
  X509v3 extensions:  
    X509v3 Basic Constraints: critical  
      CA:FALSE  
    X509v3 Key Usage: critical  
      Digital Signature, Key Encipherment  
    Netscape Cert Type:  
      SSL Client  
    Netscape Comment:  
      Certificate issued by Fermilab KCA  
    X509v3 Issuer Alternative Name:
```

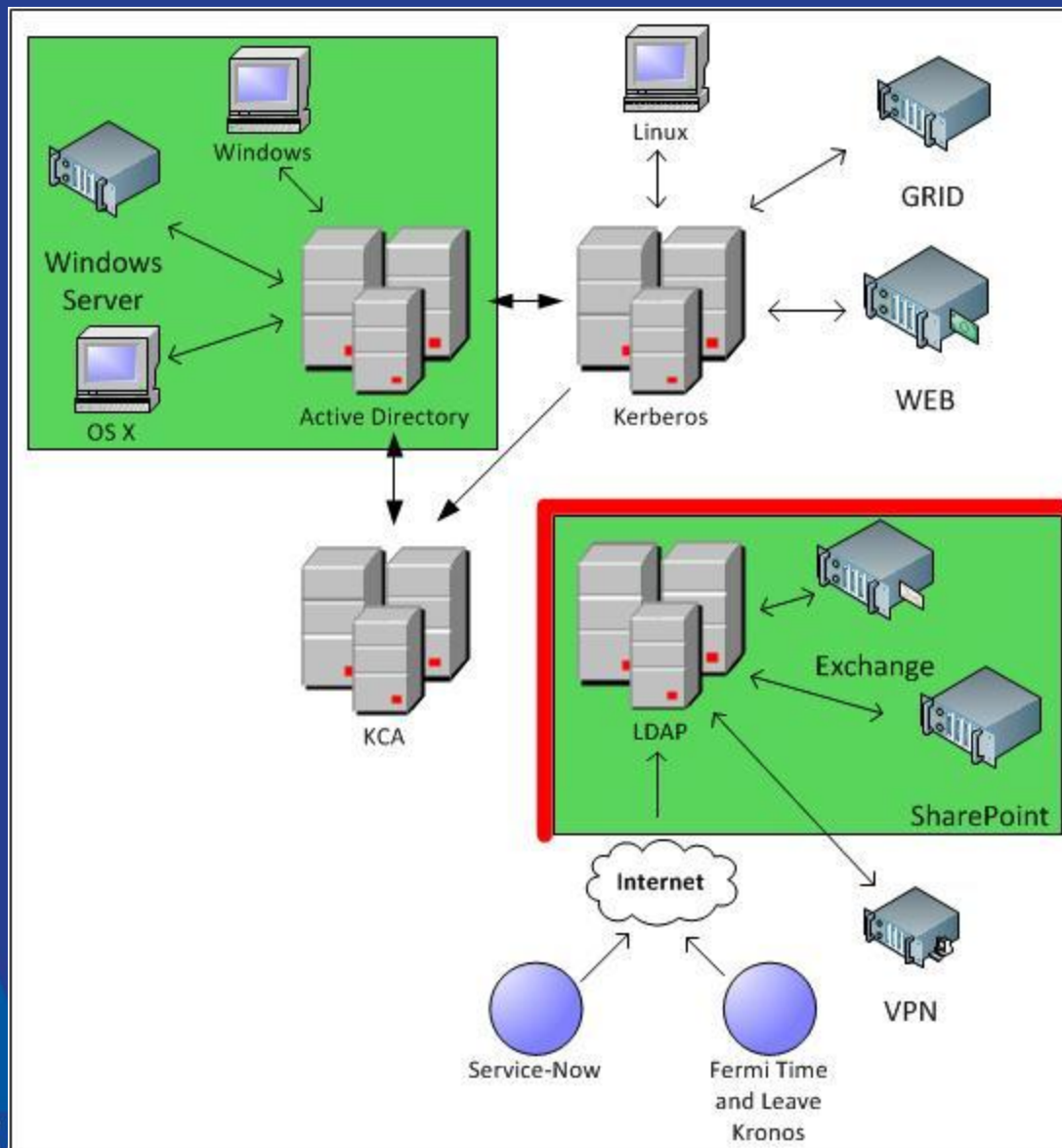
User Accounts

- All regular user accounts are created in all three authentication realms by our ID Management System
 - Active Directory
 - Kerberos
 - LDAP
- Special accounts (-admin, /admin, etc) created as necessary where needed
 - Used for delegated access to systems and services

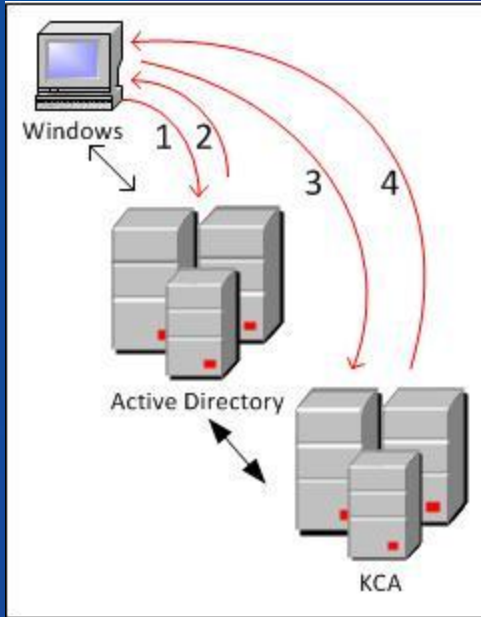
User Accounts

- Account Lifecycle
 - Creation / Termination by IdM
 - Computer Security has ability to disable user accounts
- What do we consider a user?
 - Employees
 - Contractors
 - Visitors

The Authentication Environment



Windows Logon



- Windows users authenticate against AD
 - Net ID Manager accesses KCA server on behalf of the user and gets a KCA certificate and installs it in the browser
 - Net ID Manager can manage multiple identities for the end user

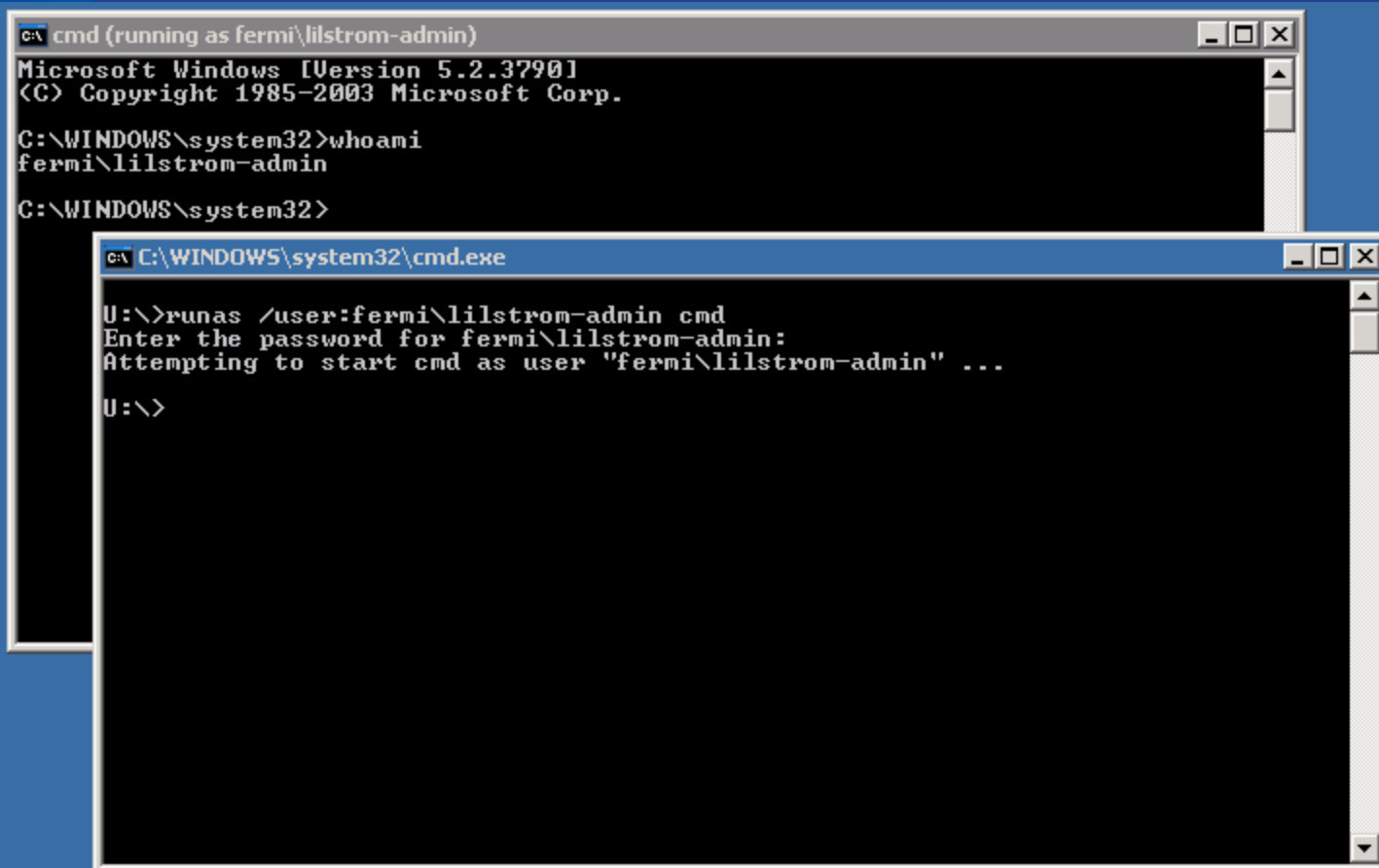
- Access to domain resources occurs as expected
 - File and print servers

Windows Logon

- Exchange
 - Separate authentication against the LDAP service
- SharePoint
 - Separate authentication against the LDAP service
- Access to Unix servers via SSH
 - Client can use Windows credentials
 - kinit against Kerberos realm and use those credentials

Windows Admin Access

- Delegated Admin
 - Log into workstation or admin terminal server with – admin credentials



```
C:\>cmd (running as fermi\lilstrom-admin)
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>whoami
fermi\lilstrom-admin

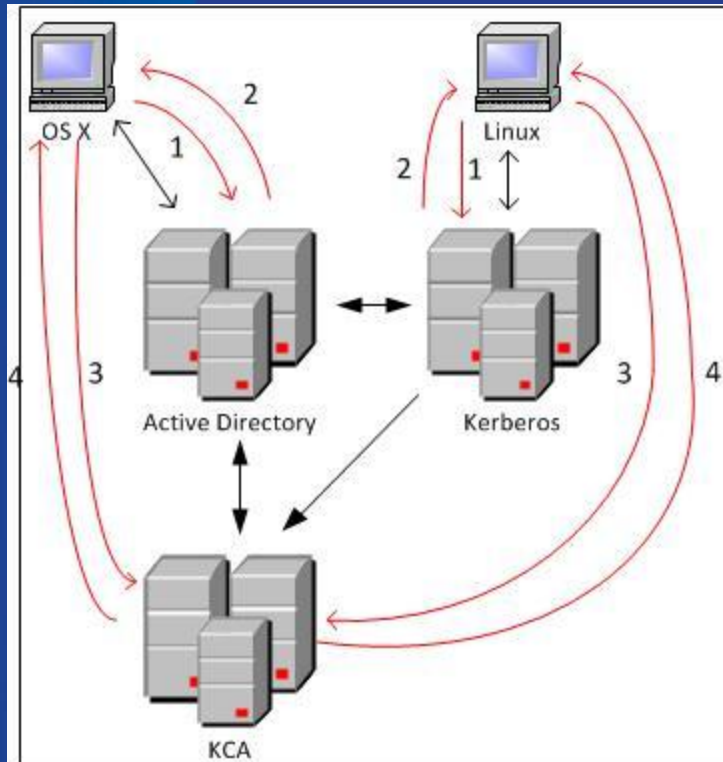
C:\WINDOWS\system32>

C:\>C:\WINDOWS\system32\cmd.exe
U:\>runas /user:fermi\lilstrom-admin cmd
Enter the password for fermi\lilstrom-admin:
Attempting to start cmd as user "fermi\lilstrom-admin" ...

U:\>
```



OS X and *nix Logon



- User Authentication
 - Local
 - Active Directory
- Get-Cert script prompts for credentials and accesses KCA server on behalf of user, gets a certificate and installs it into the browser

- SSH
 - Client uses credentials for Windows or Kerberos realm if present. Otherwise prompts for credentials.

OS X and *nix Logon

- Access to AD domain resources will prompt for credentials if necessary
- Exchange
 - Separate authentication against the LDAP service
- SharePoint
 - Separate authentication against the LDAP service

OS X and *nix Admin Access

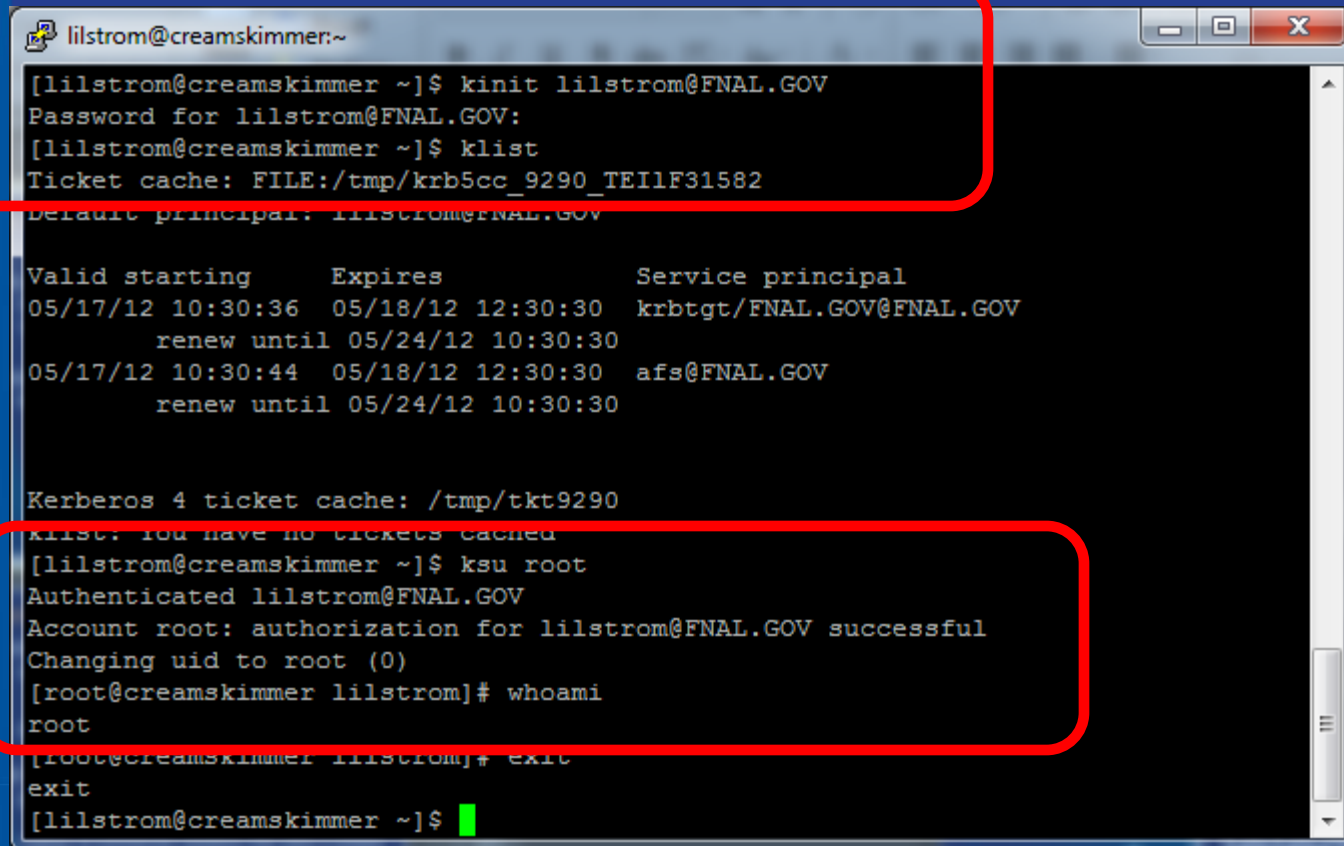
- Elevated local access
 - OS X – su and sudo
 - *nix – kinit and ksu



A screenshot of a macOS terminal window titled "tmp — sudo — 66x16". The terminal shows the following commands and output:

```
mac-116049:tmp lilstrom$ su -l lilstrom-admin
Password:
mac-116049:~ lilstrom-admin$ sudo vi /etc/krb5.conf
Password:█
```

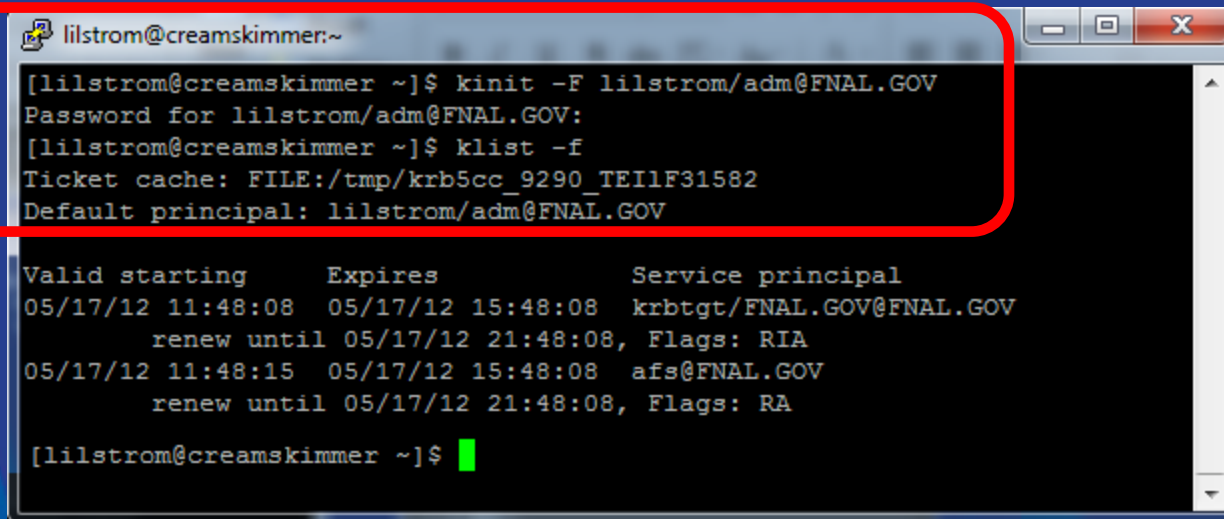
OS X and *nix Admin Access



```
lilstrom@creamskimmer:~  
[lilstrom@creamskimmer ~]$ kinit lilstrom@FNAL.GOV  
Password for lilstrom@FNAL.GOV:  
[lilstrom@creamskimmer ~]$ klist  
Ticket cache: FILE:/tmp/krb5cc_9290_TE1lF31582  
Default principal: lilstrom@FNAL.GOV  
  
Valid starting      Expires            Service principal  
05/17/12 10:30:36   05/18/12 12:30:30  krbtgt/FNAL.GOV@FNAL.GOV  
        renew until 05/24/12 10:30:30  
05/17/12 10:30:44   05/18/12 12:30:30  afs@FNAL.GOV  
        renew until 05/24/12 10:30:30  
  
Kerberos 4 ticket cache: /tmp/tkt9290  
klist: you have no tickets cached  
[lilstrom@creamskimmer ~]$ ksu root  
Authenticated lilstrom@FNAL.GOV  
Account root: authorization for lilstrom@FNAL.GOV successful  
Changing uid to root (0)  
[root@creamskimmer lilstrom]# whoami  
root  
[root@creamskimmer lilstrom]# exit  
exit  
[lilstrom@creamskimmer ~]$
```

OS X and *nix Admin Access

- Delegated Admin
 - kinit and ksu



A terminal window titled 'lilstrom@creamskimmer:~' showing the execution of 'kinit' and 'klist' commands. The 'kinit' command is highlighted with a red box. The output shows the password prompt, the successful execution of 'kinit', and the output of 'klist' showing two tickets for 'krbtgt/FNAL.GOV@FNAL.GOV' and 'afs/FNAL.GOV'.

```
lilstrom@creamskimmer:~  
[lilstrom@creamskimmer ~]$ kinit -F lilstrom/adm@FNAL.GOV  
Password for lilstrom/adm@FNAL.GOV:  
[lilstrom@creamskimmer ~]$ klist -f  
Ticket cache: FILE:/tmp/krb5cc_9290_TE1lF31582  
Default principal: lilstrom/adm@FNAL.GOV  
  
Valid starting    Expires          Service principal  
05/17/12 11:48:08 05/17/12 15:48:08 krbtgt/FNAL.GOV@FNAL.GOV  
        renew until 05/17/12 21:48:08, Flags: RIA  
05/17/12 11:48:15 05/17/12 15:48:08 afs@FNAL.GOV  
        renew until 05/17/12 21:48:08, Flags: RA  
  
[lilstrom@creamskimmer ~]$
```

Future Plans

- Federation
 - Internal Web Single Sign On (SSO)
 - Provide tokens via web form or Windows logon for web apps that support claims authentication
 - Shibboleth IdP
 - Collaboration with other InCommon members
- IdM
 - Existing IdM is home grown solution
 - Support, feature enhancement, etc
 - Looking at commercial solutions that allow a phased rollout

Future Plans

- Investigate moving *nix systems into Active Directory
- Replacement of the MIT Kerberos server infrastructure with Heimdal
- Two factor authentication

Conclusion

- Looking back at our goals:
 - We have to balance the needs for scientific computing with the needs for traditional computing
 - The solutions must be scalable and secure
 - We have to keep in mind that our real business is science
- The authentication services presented provide a secure, centralized solution that serves the needs of the Fermilab community.

Questions?